IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE EMAIL ADDRESS **'edancer223@gmail.com'** THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 5:22mj00055

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Antonio F. Davis, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with Google email address **'edancer223@gmail.com ("TARGET ACCOUNT)**, which is stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I, Antonio F. Davis, am a Special Agent Criminal Investigator with the United States Secret Service ("USSS"). I have been employed by the U. S. Secret Service since June of

2006. I have been assigned to the Washington Field Office in Washington, D.C since September of 2019. I have completed the Federal Law Enforcement Training Center's 12-week Criminal Investigation Training Program in addition to the 18-week USSS Special Agent Training Program follow-up academy. During these trainings, I have received detailed training in both academic and practical application of investigative techniques involving counterfeiting, bank fraud, wire fraud, access device fraud, money laundering, identify theft, and other financial crimes. As a federal agent, I am authorized to investigate violations of laws of the United States, and execute warrants issued under the authority of the United States.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1343 (Wire fraud), 1344 (Bank fraud), 924 (Defrauding Government of Money/Property), 1028 (Identify Theft), 1028A (Aggravated Identity Theft), 641 (Embezzlement/Stealing of United States Property), and 371 (Conspiracy to Defraud the United States); have been committed by Elizabeth Keegan. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

INVESTIGATION

The Disappearance of MP

6. During this investigation, the Woodstock Police Department ("Woodstock PD") and the USSS have developed evidence showing that from at least October, 2019 until at least October, 2021, Elizabeth Keegan hereinafter, "ELIZABETH" and others engaged in a fraud scheme involving the unauthorized access and use of financial accounts of a currently missing person ("MP") whose identity is known to investigators. ELIZABETH and others used the financial accounts and assets of MP to their own benefit. Investigators believe that this scheme involved the following manner and means:

7. On August 3rd, 2021, Sgt. Scott Miller of Woodstock PD received a call from an individual (hereafter "Witness 1") who stated that something has happened to MP, of 212 North Lee Street Woodstock, VA. "Witness 1" stated that MP's daughter, ELIZABETH, may be responsible and is now collecting money from MP as her Power of Attorney ("POA") after her believed death.

8. On August 6th, 2021, ELIZABETH told Woodstock PD that MP was living in Virginia Beach with a man named "J. F.". ELIZABETH stated MP had a cell phone with number 757-968-2173. Investigators attempted to contact this phone, it went straight to a mailbox that was not set up, indicating it was powered off.

9. A review of all of the financial accounts associated with MP suggests her financial dealings were local. MP's utility bills in the town of Woodstock were being paid through an automated process from a direct deposit from a First Bank checking account ending in 4706.

Specifically, investigators did not see any financial activity that would confirm ELIZABETH's story that MP was in fact in Virginia Beach or any other area outside of Shenandoah County, Virginia. To that end, and discussed further in paragraphs 12 and 13, the call records and cell phone location data obtained and reviewed do not suggest that MP was anywhere but Shenandoah County during times relevant to this investigation.

10. During the course of the investigation, law enforcement has interviewed several individuals close to MP and who spoke to her with some degree of regularity. An overwhelming majority of the individuals interviewed indicated they believed they had last spoken to MP in mid-to-late 2019. A review of various call records confirms that general timeframe as well. Many of these individuals suggested that MP was deceased. As to the specific whereabouts of MP, the witnesses were told various locations by ELIZABETH including that her mother, MP, was in the Netherlands, Virginia Beach, Florida, and a nursing home in Maryland. Subsequently, ELIZABETH also provided various locations, other than Virginia Beach, to investigators of the current whereabouts of her mother at various points during the investigation. As of this writing, law enforcement has not been able to verify any of ELIZABETH's explanations of MP's whereabouts as factual, nor have investigators confirmed the health and well-being of MP.

11. During various interviews with investigators, ELIZABETH also repeated the story she had originally told investigators, that MP left for Virginia Beach with "J. F.", with whom she was allegedly romantically involved in the 1970s. Investigators scoured a multitude of law enforcement databases in search of "J. F." associated with Virginia Beach. Investigators located two "J. F.s" only one of which was about the right age to have known MP in the 1970s. Law Enforcement interviewed him and his wife in reference to this investigation. "J. F." denied any knowledge of someone with MP's real name. Furthermore, investigators reviewed call

records and relevant subscriber information, which were obtained through subpoena, associated with MP's known home phone records (540-459-9100), two of MP's Consumer Cellular telephones (540-233-0225 and 540-233-2472), as well as the number provided to investigators by ELIZABETH as being MP's new cellular number (757-968-2173). The review of call records associated with these four numbers did not appear to yield any outgoing calls to or incoming calls from a telephone number associated with a "J. F.".

12. Investigators also had the opportunity to review telephonic records associated ELIZABETH. A review of ELIZABETH's cellular phone records (540-336-9954) revealed 397 communications between ELIZABETH and MP's home phone (540-459-9100) in 2019. The calls between the two were made with some degree of regularity. On or about October 10, 2019, the calls between the two abruptly ended.

13. On or about November 2, 2019, a new phone number (757-968-2173), purported to be for MP was activated on the Verizon network. This new phone number was set up with an area-code designated for Virginia Beach, Virginia (757). Theis 757 phone number, which ELIZABETH provided not only to law enforcement but also to family and friends, was purported to be the new phone number for which MP could be contacted. Investigators reviewed subscriber and other information for this new telephone number and determined that while the contact name for the new telephone number is similar to the name of MP, ELIZABETH's email address, Verizon account number, and home address were used to set up this new number with area code 757.

14. On or about November 2, 2019, ELIZABETH and the new 757 number initiated communication. From November 2, 2019 to August 23, 2020, there are only 11 individual communications between ELIZABETH's phone and the new 757 number. Despite

ELIZABETH's statements to investigators and MP's family and friends that MP is in Virginia Beach, among other places, cell tower information analyzed by investigators suggests that both ELIZABETH's phone and the device associated with the new 757 number were in the same general area, namely Shenandoah County, VA. The frequency of calls made after November 2, 2019 (when the new device associated with MP (757-968-2173) was activated) is wholly inconsistent with the frequency of calls placed by and to MP prior to October 9, 2019 (the last time that investigators know for a fact that MP was seen). Taking the aforementioned information together, investigators believe that ELIZABETH, not MP, set up the new 757 telephone number and that at all times relevant to the investigation, ELIZABETH, not MP, maintained control over the new telephone number.

15. Investigators determined that First Bank is set to foreclose on MP's residence (and belongings therein) August 23, 2022. Investigators know of no information to suggest that MP has attempted to stop or settle the foreclosure issue, nor have investigators received any information to suggest that MP has sought to reclaim any of the valuables or other items of sentimental value that would potentially be within the property.

Elizabeth Assumes Control of MP's Finances and Properties

16. Expanding on the information outlined in paragraph 14 of this affidavit, investigators reviewed the cellular phone records from the new device associated with MP (757-968-2187) and determined a phone call was placed on June 4, 2020, to Aimonetti Insurance to cancel MP's car insurance policy. During an interview with ELIZABETH, she admitted to investigators that she placed this call. Additionally, a call was placed from the new device associated with MP (757-968-2187) on June 7, 2020, to the Town of Woodstock to inquire about

tax payments on MP's properties. The Town of Woodstock employee who fielded the call remembers that it was ELIZABETH who called inquiring about the taxes on the properties.

17. Shortly after the phone call, a partial payment was made on MP's tax account with the Town of Woodstock.

18. After indicating to MP's family and friends that MP left for Virginia Beach with "J. F." (as well as telling people that MP left for the Netherlands, Florida, and a nursing home in Maryland) ELIZABETH engaged in a campaign to offload many of MP's assets. Specifically, ELIZABETH attempted to sell the SUBJECT PROPERTY and a cabin located at 3965 Moreland Gap Road New Market, VA ("Moreland Gap Cabin").

19. In order to be able to sell these two properties, ELIZABETH relied on a Power of Attorney document purporting to give ELIZABETH the authority to act on MP's behalf. During an interview with investigators, ELIZABETH stated she has other Power of Attorney documents for MP. Therefore, investigators do not believe the specific power of attorney, described further in paragraph 19, is the only forged or fraudulent document currently in ELIZABETH's possession that would give ELIZABETH rights and privileges over MP's affairs.

20. On February 22, 2021, ELIZABETH sent an email using the TARGET ACCOUNT to a realtor with a Power of Attorney document purportedly giving ELIZABETH authority to sell the SUBJECT PROPERTY and the Moreland Gap Cabin on MP's behalf. The Power of Attorney was notarized by a BB&T notary. According to the BB&T notary whose stamp and seal appeared on the Power of Attorney sent by ELIZABETH to the realtor (Witness-4), although the stamp and seal does belong to the notary, they have never worked with ELIZABETH or MP and would not notarize a document for a non- BB&T customer. In addition, the Power of Attorney document had handwritten pieces of information on it. The BB&T notary

whose stamp appeared also told investigators that such handwriting did not belong to them. Witness-4 provided emails and the Power of Attorney to law enforcement. The email to which the Power of Attorney was attached, included a footer indicating it was generated using an HP device, such as an HP printer.

21. Investigators have reviewed and analyzed financial records associated with MP during the course of this investigation. Investigators learned that MP had opened a checking account with First Bank (4706), which appeared to be MP's primary bank account. Investigators received responsive records for this account for transactions occurring between December 2018 and February 2022. Investigators observed spending irregularities for transactions that occurred after October 2019 when compared to the transactions that occurred prior to October 2019. Specifically, prior to October 2019, MP's account was debited—primarily by check-- approximately $2400 a month in specific instances that ELIZABETH is listed as the payee. In contrast, MP's account was debited—primarily by check—approximately $4,000 a month from November 2019 – December 2020 in specific instances that ELIZABETH is listed as the payee.

22. From November of 2019 to July of 2020, SON-1 (ELIZABETH'S son), whose identity is known to investigators, received a total of eight checks from MP's First Bank (4706) totaling $5,525. When investigators interviewed SON-1, SON-1 confirmed that he not only obtained the checks from ELIZABETH, but that he witnessed ELIZABETH sign MP's name as if the check was written by MP

23. Investigators also reviewed accounts held by MP and ELIZABETH with USAA. One such account was a joint account between MP and ELIZABETH (account ending in 6012). This account was established on 2/23/21 and according to ELIZABETH was set up as a place to

deposit the funds from the expected sale of the SUBJECT PROPERTY and the Moreland Gap Cabin. Investigators inquired with ELIZABETH how the account was established given the fact that she had not seen MP since fall of 2019. ELIZABETH stated she believed they opened it together over the phone. A review of ELIZABETH's phone records from February 23, 2021 (540-336-9954) indicate that she called the new 757 number associated with MP (757-968-2187) twice. However, those calls only lasted 6 and 8 seconds respectively.

24. Investigators reviewed records pertaining to a Home Equity Line of Credit (HELOC Loan) obtained by MP in October of 2018. The line of credit extended to MP was in the amount of $50,000. From the inception of the loan to about February 2021 there were regular payments made to pay down the loan. During the same time period, specifically August 5, 2019, there was a single principal advance drawn on the account by MP that was deposited in to her own First Bank Account ending in 4706. In February of 2021, there were three separate principal advances drawn on the account for a total of $5,000. Of note, these advances were made to various accounts, specifically Wells Fargo ending in 6009, Citi Cards ending in 2380, and Capital One ending in 2019. In June of 2021, there were two separate principal advances drawn on the account for a total of $3,800. Of note, these advances were made to various accounts specifically Citi Cards ending 2380 and Pentagon Federal Credit Union (PFCU) ending in 7524. A review of financial records confirms that the PFCU and Wells Fargo accounts belong to ELIZABETH. While investigators have not received information as to the account holders of the specific Citi and Capital One accounts referenced above, investigators have determined that ELIZABETH regularly makes payments to both financial institutions. Also of note, MP had never made any payments to Citi and Capital One from any account from December of 2018 (earliest financial records obtained by investigators) to February of 2021.

25. MP also had a USAA credit card. During an interview with investigators, ELIZABETH denied having access to MP's USAA credit card. However, investigators determined that certain purchases made after the fall of 2019 were not only out of the ordinary for MP's spending habits but also directly benefitted ELIZABETH and her children. Several examples of these irregular transactions include:

a. On December 16, 2019, a purchase was made in the amount of $360.80 on MP's credit card to Emmart Oil. Investigators contacted Emmart Oil who confirmed that the request for their product was made by ELIZABETH, the product was then delivered to ELIZABETH'S residence, and that while the payment was processed using MP's credit card, the transaction was logged to ELIZABETH's Emmart Oil account.

b. On December 26, 2019, a payment was made to a doctor's office in the amount of $50.81 by MP's credit card. Investigators contacted the doctor's office, who provided documentation regarding this transaction. Specifically, the payment was made for an appointment for Witness-2, who is a child of ELIZABETH. ELIZABETH and Witness-2 attended the appointment. Documentation provided by the doctor's office indicates that ELIZABETH's email, i.e. the TARGET ACCOUNT, was listed on the consent form.

c. On January 13, 2020, a payment was made to a veterinarian in the amount of $100 by MP's credit card. Investigators contacted the veterinarian's office who explained that payment was made for dental work on ELIZABETH's dog.

d. On July 24, 2020, a payment was made to Tractor Supply Co. in the amount of $849.99 by MP's credit card. Investigators contacted Tractor Supply Co. who

explained that while MP's card was used to make the purchase, the purchase was logged to ELIZABETH's Tractor Supply Co. account with ELIZABETH's home address and phone number associated with it.

Federal Funds Fraud

26. When MP's husband passed away in 1993, her husband's retirement funds through the Defense Finance Accounting Service ("DFAS") were redesignated to MP. A review of the financial accounts for MP determined she was receiving approximately $6400 a month from DFAS. These monthly deposits were made to MPs First Bank Account (4706), first refenced in paragraph 9 above. Investigators contacted DFAS and determined that approximately $150,000 had been deposited in to MPs First Bank account from October 2019 – August 2021.

27. Investigators reviewed MP's financial accounts and determined three payments were deposited into MP's First Bank account (4706) by the Internal Revenue Service between April 2020 and April 2021. These payments totaled $3,200.

28. Additionally, investigators reviewed MP's financial accounts and discovered monthly payments of Social Security funds deposited in to MP's First Bank account (4706). From October 2019 (the last time that investigators know for a fact that MP was seen) until August 2021 the account received approximately $25,623.55.

29. From October 2019 until the time in which investigators contacted the relevant federal agencies of the alleged embezzlement scheme, over $170,000 had been deposited in federal funds into MP's First Bank account (4706).

30. As of January 2022, this First Bank account (4706) was drained and is currently in a negative balance. Examples of unusual payments from this bank account (4706) to ELIZABETH and SON-1 are described above in paragraphs 21 and 22.

ADDITIONAL INFORMATION REGARDING THE TARGET ACOUNT

31. There is probable cause to believe that at times relevant to the investigation, not only did ELIZABETH have control and access over the TARGET ACCOUNT but the TARGET ACCOUNT was used in furtherance of the scheme to defraud both MP and the United States.

32. In addition to the information set forth above in paragraphs 17-19, while logged in to her google profile edancer233@gmail.com, associated with the TARGET ACCOUNT, ELIZABETH made the following queries:

- "Find Frances Keegan Amsterdam" – 5/6/22
- "Gated Community Virginia Beach VA" – 10/10/19
- "Frances Keegan" (peoplelooker.com) – 5/6/22

33. During a search of ELIZABETH's electronic devices pursuant to a search warrant, investigators identified software being used on two Dell tablets that has the capability to permanently erase much of the data (browsing history, location information, etc.) on the particular device, but would not erase the data from Google's servers. Forensic examination showed that ELIZABETH operated the TARGET ACCOUNT from both of these Dell tablets. Investigators were able to recover partial data from these Dell Tablets devices, but significant gaps of information exist in the forensic examinations conducted by investigators consistent with data being permanently erased by this software.

34. Additionally, investigators determined during the aforementioned forensic examination that location services had been disabled on ELIZABETH's two Android cellular phones, each of which used the TARGET ACCOUNT as a login to access the phone. devices.

35. There is therefore probable cause to believe that evidence of the crimes and schemes described above deleted or disabled from the Dell tablets and Android phones can be recovered from the Google server.

BACKGROUND CONCERNING GOOGLE[1]

36. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

37. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android

[1] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

38. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

39. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

40. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

41. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone

number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

42. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

43. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

44. Google maintains location information for those devices that either run a Google-based operating system or have an application, such as Gmail, downloaded to it. This information is relevant in determining where a particular user was at a given time.

45. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why,

when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

46. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

47. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

48. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a

plan to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

49. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

50. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

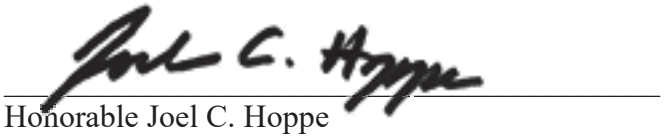
51. Based on the forgoing, I request that the Court issue the proposed search warrant.

52. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/Antonio F. Davis
Antonio F. Davis
Special Agent
United States Secret Service

Received by reliable electronic means and sworn and attested to by telephone on August 22nd, 2022.



Honorable Joel C. Hoppe
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated **Edancer233@gmail.com** ("the Target Account") that is stored at premises owned, maintained, controlled, or operated by Google LLC a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google. Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from **September 1, 2019 to present** unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
6. To the extent such records exist, any query history done on a device-supported browser while logged into the Target Account
7. To the extent such records exist, location information in the form of Global Positioning System (GPS) coordinates while the device was running any Google-supported application, feature, or operating system.
8. All emails, including inbox, outbox, sent, and deleted emails, stored on Google's servers for the Target Account for the requested time period.

9. E-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services including but not limited to incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic communications; attachments to communications (including native files); source and destination addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies); Length of service (including start date and creation IP) and types of service utilized.

10. All records and other information concerning any document, or other computer file created, stored, revised, or accessed in connection with the Target Account or by an Account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

11. Records and other information concerning any document, or other computer file created, stored, revised, or accessed in connection with the Account or by an Account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

12. All Google Voice Account information, including voice specific subscriber information (for example, signup IP and associated timestamp, and user-provided name), all account settings and account change history, and the contents of all voicemail messages and text messages;

13. Means and source of payment (including any credit card or bank account number); and

14. Change history.

b. All device information associated with the Target Account, including but not limited to, manufacture names, model numbers, serial number, media access

control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs

Google is hereby ordered to disclose the above information to the government within 14 DAYS days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits or instrumentalities of violations of 18 U.S.C. §§ 1343 (Wire fraud), 1344 (Bank fraud), 924 (Defrauding Government of Money/Property), 1028 (Identify Theft), 1028A (Aggravated Identity Theft), 641 (Embezzlement/Stealing of United States Property), and 371 (Conspiracy to Defraud the United States), including but not limited to:

a. Communications in ay form between ELIZABETH and MP;

b. Communications in any form between ELIZABETH and co-conspirators known or unknown;

c. Communications with financial institutions, real estate institutions and/or regarding any financial transactions, real estate transactions, assets of MP, assets of ELIZABETH, taxes.

d. Any and all financial records;

e. Information regarding the whereabouts of MP; any communications or data of any kind regarding ELIZABETH's knowledge of MP's whereabouts;

f. Powers of Attorney, communications regarding powers of attorney or accounts opened under MP's name, data of any kind regarding accounts opened under MP's name;

g. Information regarding the use of MP's financial accounts or other assets;

h. Evidence indicating how and when the Target Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

i. Evidence indicating the Account owner's state of mind as it relates to the crimes under investigation;

j. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).